TITLE OF THE INVENTION:

METHOD AND APPARATUS FOR TRANSMITTING DATA SUBJECT TO PRIVACY RESTRICTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS:

**[0001]** This application claims priority of Provisional Patent Application Serial No. 60/427144, filed November 15, 2002, the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION:

Field of the invention:

**[0002]** The invention relates to data storage and retrieval, and more specifically to granting permissions to operate on data on machines separate from an originating storage. In particular, the invention relates to data transfers between a service provider and a user or to peer-to-peer data transfer, where a user communicates with another user, wherein one of the users acts as a "service provider."

Description of the related art:

**[0003]** Users may be provided with various types of services via a communication system. The communication system can be seen as a facility that enables communication between two or more entities such as user equipment and/or networks entities or other nodes associated with the communication system. The communication may include, for example, communication of various kinds of data such as voice data, electronic mail (email), text messages, content data, multimedia and so on.

**[0004]** A party of a communication may require privacy or other security features. For example, personal information may be suppressed entirely or partly from another party of the communication. The party requiring the privacy may typically be a user or a consumer of a service provided by a service provider (SP). A service provider may be an entity that is connected to

one or more communication systems, for example, the Internet or other data network. The service provider may also be implemented as a part of a communication system. The service provider may also be another user acting as a service provider. Other parties may include, but are not limited to, the intended destination of a message, such as the service provider, or an intermediary handling this message.

**[0005]** Service providers in the Internet may have privacy policies that are posted on their web sites and which provide some protection. All service providers do not have privacy policies. Even if a service provider has a privacy policy, it can change the policy after the user has released data to the service provider. The user has no easy way of comparing service providers' privacy policies. Furthermore, the user has no way to prove under which policy he has provided data to a service provider.

**[0006]** Privacy policies may be based on any appropriate protocol, such as the Platform for Privacy Preferences (P3P) protocol. P3P enables Web sites to express their privacy policies in a standardized format that can be downloaded and read by web browsers and other end-user software tools. These end-user software tools can display information about site's privacy policy to users and take actions based on a user's preferences. Such end-user software tools might provide positive feedback to users when the sites they visit have privacy policies matching their preferences, and provide warnings when a mismatch occurs. The end-user tools may also notify users when a site's privacy policy changes.

**[0007]** In the known solutions, it is hard to check and find a privacy policy matching since virtually every service provider has its own privacy policy. As every service provider has a different privacy policy, it is very difficult for the user to get an overview of different service provider's privacy policies and to compare them.

**[0008]** There is also a need for an improved system for testing the privacy

policy matching or otherwise testing that the privacy levels are acceptable for the parties involved or for other such functions. Furthermore, certain applications may require a system enabling the use of different privacy policies with different service providers. It might also be advantageous in certain applications to be able to track later the policy under which the data of the user was released to a certain service provider at a certain moment. In certain embodiments, it might be advantageous to attach a reference to the agreed upon privacy policy to the data that is released.

SUMMARY OF THE INVENTION:

**[0009]** According to an embodiment of the invention, there is provided a method for controlling transfer of data between a provider and a user in a communication system where the provider possesses a privacy policy. The method includes the steps of introducing to a broker a usage policy for the constraints related to the data of the user, receiving a request for data associated with the user from the service provider to the broker, checking in the broker the request against the usage policy of the user, and deciding if the data can be released.

**[0010]** In another embodiment, the usage policy for the constraints related to the data of the user is preferably defined by the user. The user may define a strictness level for his usage policy describing constraints related, for example, to the constraints related to the data of the user, such as purpose of use, retention and so on. The user may define the usage policy by means of a predefined set of policies. For this, standardized privacy policies or privacy contracts known by both the service provider and the user may be used. Thus the usage policy of the user is preferably defined by the same elements than the privacy policy of the service provider. The user may also define an acceptable usage policy in a general manner to be respected in relation to any service provider. Such a general acceptable usage policy may then be mapped to a predefined set of policies. A similar mapping mechanism may be carried out for the privacy policy of a service provider to find a common privacy

policy. Alternatively, the user may define his usage policy in function of the service provider so that the data to be released may vary between each service provider or each type of service provider. In such a case, the data to be released may refer to an attribute, such as an address, or to a set of attributes, such as a name and an address. The broker may be configured to host the privacy policies and the usage policies. The broker may also carry out the mapping of the policies defined by the user and the service provider, when mapping is required. A negotiation mechanism may be used for the release of data. In certain embodiments, the privacy policies or usage policies may be attached to the released data.

**[0011]** In certain embodiments of the invention the user may easily compare the privacy policies of service providers since they use the same set of policies. In certain applications, the user may attach an electronically signed, legally binding usage policy, i.e. a privacy policy defined by the user, to the data of the user when the data is released to the service provider.

BRIEF DESCRIPTION OF THE DRAWINGS:

**[0012]** The invention will now be described in further detail, by way of example only, with reference to the following examples and accompanying drawings, in which:

**[0013]** Figure 1 shows an example of an arrangement in which the invention may be implemented;

**[0014]** Figure 2a shows an example of a collection of attributes defining the strictness level 1, "Privacy Strict", of the privacy policy or usage policy in accordance with one embodiment of the invention;

**[0015]** Figure 2b shows an example of a collection of attributes defining the strictness level 2, "Privacy Cautious", of the privacy policy or usage policy in accordance with one embodiment of the invention;

**[0016]** Figure 2c shows an example of a collection of attributes defining the strictness level 3, "Privacy Neutral", of the privacy policy or usage policy in accordance with one embodiment of the invention;

**[0017]** Figure 2d shows an example of a collection of attributes defining the strictness level 4, "Privacy Flexible", of the privacy policy or usage policy in accordance with one embodiment of the invention;

**[0018]** Figure 2e shows an example of a collection of attributes defining the strictness level 5, "Privacy Casual", of the privacy policy or usage policy in accordance with one embodiment of the invention;

**[0019]** Figure 3 shows a binding profile describing access and policy of a personal profile of a user in accordance with one embodiment of the invention;

**[0020]** Figure 4 shows a flow chart of the method of the invention;

**[0021]** Figures 5a, 5b and 5c show message sequence charts describing ways of handling attribute request and checking of privacy policies and usage policies in accordance with certain preferred embodiments of the invention; and

**[0022]** Figure 6 shows a message sequence chart describing a way of handling attribute request and checking of privacy policies and usage policies in accordance with another embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS:

**[0023]** Figure 1 shows an example of an arrangement including a data communication network 10, a plurality of service providers (SP) 12, 14 and 16, and a plurality of end-users 18, 20 and 22. In connection with the invention, the term "service provider" typically means a system for providing services, such as sales, information distribution or any other form of service provisioning that may occur via a communication network. Service provider may also be another end-user. The service provider may also act in certain

circumstances as a "Web Services Consumer." A set of service and identity providers having a business relationship may form a Circle of Trust (CoT).

**[0024]** The communication network 10 may be any appropriate data communication network. In one embodiment, the communication network is provided by the Internet. The terms "user", "end-user" and "principal" refer to a subject, such as a person, a company, a system or a device, requiring a service provided by the service provider. It shall be appreciated that Figure 1 is only an example showing three service providers and end-users and that the number of these entities may differ substantially from that which is shown.

**[0025]** Figure 1 shows also a broker entity 24 configured for operation in accordance with the invention. The broker entity 24 is provided with appropriate devices for the provision of data storage and processing facilities 26 and 28, respectively. The operation of the exemplifying broker entity 24 will become clear from the description of the embodiments of Figures 2 to 6.

**[0026]** It is to be noted, that the term "broker" is used herein to describe any network entity or an entity associated with the user being capable to represent the user in the data transfer transaction. The broker may also be referred to as a Web Service Provider (WSP) capable of accomplishing the privacy control functions as described herein. The Web Services Provider provides services to the above-mentioned "Web Services Consumer." The broker may be located in the network or in the user terminal, for example.

**[0027]** The service provider or the Circle of Trust 12, 14, 16 preferably has a predefined set of privacy policies. These privacy policies may include information such as intended usage, retention, sharing and so on. Preferably, the privacy policies are sequenced according to strictness. The strictness may be an arbitrary metric assigned to a collection of privacy attributes such that higher levels of strictness are assigned values that are higher than lower levels of strictness. It is also possible in certain applications, that the privacy policy of the service provider is undefined.

**[0028]** A user or a principal 18, 20, 22 may define or choose constraints related to his data. The user may, for example, define one or more policies that are acceptable for the release of a specific attribute or class of attributes and for each service or category of services. The user may define to whom and according to what policy data may be released. Usage policies may also describe restrictions related to the use of attribute data. The user may define how the data can be used, with whom the data can be shared, for how long the data can be retained and so on. The data can be any attribute or set of attributes associated with the user, such as name, address, other contact information, profession, payment information, sicknesses, hobbies, preferences or any other data relating to the user.

**[0029]** The user may alternatively choose a default policy that applies for all categories. According to the invention, the privacy policy of the user may also be termed as a "usage policy." The usage policy may include similar information elements than the privacy policy of a service provider. In one embodiment, the user and the service provider use the same predefined set of policies including the same information elements and set of values.

**[0030]** For example, in an embodiment of the invention, the service provider 12, 14, 16 may ask for attributes related to a user 18, 20, 22. At the same time, the service provider preferably indicates its privacy policy. A broker 24 may then check the privacy policy of the service provider against the usage policy requirement defined by the user for the attributes in question. If the privacy policy of the service provider is equal or more restrictive than the usage policy defined by the user, the requested attribute data is released. If the privacy policy of the service provider is less restrictive than the usage policy, the user may be warned. The user may be asked if he wants to provide the requested data and continue the use of the service, or end the session.

**[0031]** An example of a possible set of different privacy or usage policies that reflect different degrees of strictness is given in figures 2a-e by defining

five strictness levels, which may be ranked in order: level 1 - privacy strict (Fig. 2a), level 2 - privacy cautious (Fig. 2b), level 3 - privacy neutral (Fig. 2c), level 4 - privacy flexible (Fig. 2d), and level 5 - privacy casual (Fig. 2e).

**[0032]** Each privacy or usage policy may include for example following elements or attributes:

- "Purpose" describing the purposes of data collection or uses of data;
- "Recipient" describing the recipients of the collected data;
- "Retention" indicating the retention policy that applies to the data;
- "Non-identifiable" signifying that no data is collected or that all of the data referenced will be made anonymous upon collection;
- "Access" indicating whether the service provider provides access to the collected data;
- "Disputes" describing dispute resolution procedures that may be followed for disputes about a services' privacy practices; and
- "Remedies" specifying the possible remedies in case a policy breach occurs.

**[0033]** Typically the elements (e.g. purpose, recipient and so on) defining the privacy policy or the usage policy have an acceptable preset value or a set of acceptable preset values. Values of the elements in the level 1 "privacy strict" policy are typically very restrictive, whereas the values of the level 5 "privacy casual" may be very permissive. The privacy or usage policies may be arranged into an ordered set. The policies may be ordered, for example, according to the strictness level or according to any other appropriate criteria.

**[0034]** As mentioned above, in one embodiment, the user and the service provider may use the same set of policies including the same elements and set of values. In other words, the privacy policy and the usage policy preferably refer to similar set of policies. In another embodiment, the set of policies is arranged in an order as explained above. The term "privacy policy" is used in

this description to denote a privacy policy defined by the service provider and term "usage policy" is used to denote a privacy policy defined by the user. In this embodiment the comparison of policies may be carried out directly without any preceding mapping of policies.

**[0035]** Figure 3 shows an example of a binding profile describing access and policy of personal profile of a user or a principal. The profile may be a database of fields that match an attribute or set of attributes 601 of the user to a service provider 603 and usage policy 604. The profile may be stored in the broker or may be accessible to the broker.

**[0036]** The arrangement of Figure 1 is used here as an example of a system where the invention may be implemented. A user 18, 20, 22 may contact a service provider 12, 14, 16 and request a service. Below, an example is described with reference to a user 18 and a service provider 12. It should be noted, that this is not meant to limit by any means the number or nature of the user or the service provider.

**[0037]** In the arrangement of Figure 1, a broker 24 may collect information relating to the user privacy, such as user consent, access rules and usage policy. The broker 24 represents the user 18 in the transaction for transferring data between the service provider 12 and the user 18. The service provider 12 may then send to the broker 24 a request for data associated with the user 18. The service provider 12 typically needs this data to proceed with the request of the user 18.

**[0038]** The above procedure is shown in a flow chart in Figure 4. The usage policy of the user is introduced in the broker (step 1). The broker receives a request for data associated with the user from the service provider (step 2). The broker checks the request against the usage policy of the user (step 3). Following the checking, it is decided if the requested data can be released (step 4).

**[0039]** In another embodiment, the request includes the following elements: an identifier of the user; at least one descriptor of the data sought by the service provider and an indicator of the privacy policy or privacy assurance in effect at the service provider for which the service provider makes an assurance that it will be applied to any data returned by the broker. Such a privacy assurance may have been pre-selected by the service provider from a range of privacy polices or privacy assurances.

**[0040]** The broker may make a check of the privacy policies or usage policies stored within itself or its domain or a place in the networks specified by a Uniform Resource Locator (URL) address. The broker may compare the indicator of the privacy policy of the service provider to the usage policy associated with data of the user that meets the description of the descriptor. The usage policy may have been previously associated with the data by earlier actions of the user. Such a check, or determining step, may be a comparison of a criterion such as policy strictness or a privacy attribute of a privacy policy of the service provider carried in the request.

**[0041]** The criterion is met for example if the privacy policy indicated in the request equals the usage policy of the user. In case the criterion is met, the broker may send at least one datum to the service provider. The at least one datum sent to the service provider is the counterpart to the descriptor included in the request. Such a response by the broker may satisfy the basic query for data that fits or otherwise is looked up based on the descriptor and the identifier of the user.

**[0042]** Failure of the request occurs when the broker makes a determination that a privacy assurance of the service provider is below a criteria previously established by the user associated with the data fitting the attributes of the request. In other words, failure of the request occurs when the privacy policy of the request does not equal or is less strict than the usage policy of the user

stored in the broker. A response may include indication of an acceptable usage policy.

**[0043]** Alternatively, the broker may transmit a response bearing an error indicator or invoke an interaction service to check if the user wants to change his policy preference. It is thus indicated in the response that a privacy assurance is below or not equal to a criteria previously established by the user associated with the data fitting the attributes of the request.

**[0044]** In another embodiment, a service provider makes a request to the broker. The request may include an identifier of a user or a principal and at least one descriptor of the data sought by the service provider. The broker may make a check of the privacy policies or the usage policy of the user stored within itself or its domain or a place in the networks specified by a URL address, the check being associated with the at least one descriptor. The broker may then send a response including at least one datum corresponding to the query for data that is looked up based on the at least one descriptor. Additionally, the response typically includes the at least one usage policy that had been previously set by the user for that at least one datum.

**[0045]** The service provider may evaluate the usage policy according to the criteria in effect that moment at the privacy policies of the service provider. Such an evaluation may result in the service provider transmitting an error message. In addition to an error flag, such an error message may include an assurance that the data is being deleted or otherwise discarded.

**[0046]** The broker may transmit an error acknowledgement which may include messages, such as "error received" and "acknowledge receive discard data indication." Any other messages may also be included in the response depending on the situation. Configuration of these different messages is not limited to the examples given in this text.

**[0047]** The broker may also attach an electronically signed usage policy to the data of the user when the data is released to the service provider. The user may sign electronically his usage policy in any appropriate way.

**[0048]** Figures 5a, 5b and 5c show signaling flows for some embodiments in accordance with the invention for attribute or data request and checking of privacy policies and usage policies. The privacy policy including for example intended usage set by the service provider 12 may be defined in the request 901, 911, 921. The usage policy required by the user is given in the response 902, 912, 922. In a successful case the privacy policy of the request 901, 911, 921 and the usage policy of the response 902, 912, 922 must match. This means that the usage policy of the user must define values for the attributes comprised in the request 901, 911, 921. In a successful case, the value defined by the user must be the same or less restrictive than the value required by the service provider.

**[0049]** In the example of Figure 5a, the service provider 12 may request for example the name and the address of the user with PrivacyPolicy_2 (privacy cautious). The user setting for the usage policy is, in this example, UsagePolicy_2. The broker 24 then discloses the user name and address using UsagePolicy_2.

**[0050]** In the example of Figure 5b, the service provider 12 may request for example the name and the address of the user with PrivacyPolicy_5 (privacy casual). The user setting for the usage policy is UsagePolicy_2 (privacy cautious). The broker 24 may disclose name and address using only UsagePolicy_2. The broker 24 may also indicate in the response that there was a mismatch between the privacy policy and the usage policy. Alternatively, the broker 24 may simply indicate that the required level of the privacy policy is not acceptable, as shown in the example of Figure 5c.

**[0051]** Figure 6 shows a situation, when the request 931 does not define the privacy policy level and thus indicates no intended usage. The usage policy is

given in the response 932. In this embodiment, the service provider 12 must respect these directives. It is possible, however, that the service provider is not able to respect the level of the usage policy required by the user 18. In that case, the service provider may send to the broker 24 another request 933 including an indication that the required usage policy may not be respected. The broker 24 may, in its response 934, indicate a requirement for further action. Further action, for example, may be to discard the data.

**[0052]** In the embodiments shown in figures 5a-c and 6, the privacy policies and usage policies are as defined above. The service provider 12 sets or chooses among a well known set of policies the privacy policy and the user or principal 18 sets or chooses the usage policy as mentioned above. In accordance to the invention, the usage policy is stored in a broker 24. The broker 24 can decide to disclose attributes only when the usage policy is equal or less strict to the privacy policy the service provider indicated in the request. In case the usage policy is less strict, the broker 24 may disclose attributes using the usage policy equal to the privacy policy given in the request of the service provider. The broker 24 should not change the usage policy defined by the user to attribute association without asking for user consent.

**[0053]** In one embodiment, either the Circle of Trust (CoT) or Liberty has a web site where the five above defined policies are available online. Alternatively the policies can be located at an entity that provides a well known set of policies for a number of CoTs. The message may carry for example an indication, such as "CoTPrivacyUsagePolicyURL" or "LibertyV2.0PrivacyUsagePolicyURL".

**[0054]** Advantageously, several service providers or sets of service providers may use the same set of policies.

**[0055]** Although the invention has been described in the context of particular embodiments, various alternative embodiments are possible. For example, even if the communication network described in the examples above is mainly

the Internet, the invention may be carried out in any other communication network. Examples of other networks may include, but are not limited to, other packet switched networks such as the third generation wireless network technologies like Wideband Code Division Multiple Access (WCDMA), CDMA2000, Universal Mobile Telecommunication System (UMTS) and Enhanced Data rates for GSM Evolution (EDGE). Networks may also include cellular networks such as the public switched telephone network.

**[0056]** In certain embodiments, it is also possible that the user carries out the function of the service provider and the service provider is functioning in place of the user. The terms service provider and user thus describe the function of the entity in question.

**[0057]** Thus, while the invention has been particularly shown and described with respect to specific embodiments thereof, it will be understood by those skilled in the art that changes in form and configuration may be made therein without departing from the scope and spirit of the invention.